58

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/724,187	11/27/2000	Todd Bartleson	NAI1P137/00.123.01	7757

28875 7590 01/13/2005

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
AKPATI, ODAICHE T	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 01/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/724,187	BARTLESON ET AL.	
	Examiner	Art Unit	
	Tracey Akpati	2135	

-- Th MAILING DATE of this communication appears on th cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 July 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,7-14,17 and 20-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,7-14,17 and 20-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 November 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5)☐ Notice of Informal Patent Application (PTO-152)
6)☐ Other: _____.

DETAILED ACTION

1. Claims 1-4, 7-14, 17, 20-25 are pending. Claims 1, 13, 14, 17 and 20 have been amended. Claim 6, 16 and 18 has been cancelled. Claims 21-25 has been added. The amendments have necessitated a final rejection.

Response to Arguments

Applicant's arguments filed 7/15/04 have been fully considered but they are not persuasive.

2. *The attorney argues that Atkinson et al does not suggest 'monitoring calls to applications' nor 'temporarily preventing an action ...from being executed if the identified code does not correspond to a code associated with data said action is to be performed upon.'* Atkinson et al (abstract) discloses embedding of a certification within an executable file so as to ensure the authenticity of that file. When the file is received, the embedded code is authenticated by the client. Hence monitoring of the calls (i.e. requests sent to the client) is performed. If the code received at the client is positively authenticated, the requested action can be performed. If authentication fails, the requested action is prevented (Atkinson et al, column 2, lines 44-52; column 3, lines 14-24).

2. *The attorney argues that Atkinson in no way suggests applicant's "trusted applications."* Atkinsn discloses certain applications (i.e. downloaded code or executable file) whose integrity is trusted because the identity of the publisher rather than the actual code is authenticated. Hence these applications suffice as trusted applications.

3. *The attorney argues that Chess does not disclose the limitations of claims 9-12 namely 'wherein the action requested is a password manipulation', 'deletion of data' and 'manipulation of an operating system.'* Chess meets this limitation on column 1, lines 49-55 and on column 2, lines 8-13. Chess discloses discrimination of malicious changes to digital information (title). It accomplishes this by deciding if a change to one or more objects was caused by normal system operation or by a malicious program. This fully meets the limitation of Claim 9-12 which all disclose various malicious operations.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 8, 13, 14, 17, 20, 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Atkinson et al (6367012 B1).

With respect to Claim 1, the limitation of "monitoring calls to applications resident on the handheld computer" is met on column 2, lines 35-40 and 44-52; and "identifying a code associated with a program initiating said call" is met on column 3, lines 13-24; and "at least temporarily preventing an action requested by said call from being executed if the identified creator code does not match a creator code associated with data said action is to be performed upon" is met on column 9, lines 9-20; and "wherein identifying a code comprises identifying a creator code on a handheld computer operating system; wherein the creator code is used to

prevent malicious behavior" is met in the abstract; "wherein at least one of the applications is identified as a trusted application; wherein the trusted application is not prevented from performing actions even if the creator code associated with the trusted application does not match the creator code associated with the data said action is to be performed upon" on column 3, lines 18-24. The signature/certificate represents the creator code because it verifies the integrity and authenticity of the file/program being downloaded to the computer so as to prevent any kind of malicious behavior/code.

It would have been obvious to have a handheld computer in place of the computer disclosed in Atkinson et al because a handheld computer is simply a computer, with all its working properties and capabilities, but shrunk in size. Moreover, according to In re Rinehart, 531 F.2d 1048, 189 USPQ 143 (CCPA 1976), 'the mere scaling up of a prior art process capable of being scaled up, if such were the case, would not establish patentability in a claim to an old process so scaled.' 531 F.2d at 1053, 189 USPQ at 148.

With respect to Claim 8, the limitation of "asking a user whether to accept said data before loading said data onto the handheld computer" is met inherently n column 9, lines 9-20. The handheld device is obvious for the reasons disclosed in Claim 1.

With respect to Claim 13, the limitation of "monitoring requests for action by applications on the handheld computer" is met on column 2, lines 35-40, 44-52; and "evaluating said requests to determine if said requests may result in potentially harmful behavior to data stored on the handheld computer" is met on column 2, lines 35-40, 44-52; and "preventing said

action from being performed if one of said requests for action is identified as potentially harmful behavior" is inherently on column 3, lines 47-58; and "notifying a user of the handheld computer of said potentially harmful behavior" is met on Fig. 6; and "wherein evaluating said requests comprises comparing a creator code associated with the application requesting said action with a creator code associated with data the action is to be performed upon; wherein the creator code is used to prevent malicious behavior" is met on column 3, lines 14-24; and "wherein at least one of the applications is identified as a trusted application; wherein the trusted application is not prevented from performing actions even if said one request is identified as potentially harmful, if requested by the trusted application" is met on column 2, lines 6-11; column 3, lines 47-54

The signature/certificate represents the creator code because it verifies the integrity and authenticity of the file/program being downloaded so as to prevent any kind of harmful behavior/code.

It would have been obvious to have a handheld computer in place of the computer disclosed in Atkinson et al because a handheld computer is simply a computer, with all its working properties and capabilities, but shrunk in size. Moreover, according to In re Rinehart, 531 F.2d 1048, 189 USPQ 143 (CCPA 1976), 'the mere scaling up of a prior art process capable of being scaled up, if such were the case, would not establish patentability in a claim to an old process so scaled.' 531 F.2d at 1053, 189 USPQ at 148.

With respect to Claim 14, the limitation of "wherein monitoring requests for action comprises monitoring API calls" is met on column 26, lines 7-17, 26-39; column 30, lines 27-33.

With respect to Claim 17, its limitation is similar to Claim 1 limitation and hence its rejection can be found therein.

With respect to Claim 20, its limitation is similar to Claim 13 limitation and hence its rejection can be found therein. The added limitation of "wherein at least one of the applications is identified as a trusted application; wherein the trusted application is not prevented from performing actions even if the creator code associated with the trusted application does not match the creator code associated with the data said action is to be performed upon" is met on column 3, lines 18-24.

With respect to Claim 25, the limitation of "wherein an efficient detection of viruses is provided for the handheld computer without sacrificing limited memory of the handheld computer" on column 2, lines 35-52.

Claims 2-4, 23-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Atkinson et al (6367012 B1) in view of Walsh et al (5956481).

With respect to Claim 2, all the limitation is met by Atkinson et al except for the limitation disclosed below.

The limitation of "wherein monitoring calls to applications comprises installing a patch on the handheld computer, the patch being operable to intercept calls" is met on Walsh et al on column 2, lines 6-16.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Walsh et al within the system of Atkinson et al because installing a patch will enable the computer processes to execute the patch in place of the original, less secure routines in order to ensure the system is immune from malicious attack/code.

With respect to Claim 3, all the limitation is met by Atkinson et al except for the limitation disclosed below.

The limitation of "wherein installing a patch comprises replacing an API address with a patch address" is met by Walsh on column 2, lines 6-16.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Walsh et al within the system of Atkinson et al because replacing an API address with a patch address will enable the computer processes to execute the patch in place of the original, less secure routines in order to ensure the system is immune from malicious attack/code.

With respect to Claim 4, all the limitation is met by Atkinson et al except for the limitation disclosed below.

The limitation of "wherein installing a patch comprises utilizing get trap and set trap commands" is inherently met by Walsh on column 2, lines 6-16.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Walsh et al within the system of Atkinson et al because the trap commands are inherent routines executable with a patch, enabling the patch to do its job.

With respect to Claim 23, all the limitation is met by Atkinson et al except for the following limitation.

The limitation of "wherein the temporary prevention of the action requested by said call involves notifying a user that the potentially harmful action has been requested and giving the user a plurality of options selected from the group consisting of allowing one of the applications to continue with the action, always allowing one of the applications to perform the action, and preventing one of the applications from performing the action" is met by Walsh on column 9, lines 56-67; column 10, lines 1-12, 35-42.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Walsh et al within the system of Atkinson et al so as to prevent a malicious program from being downloaded onto the client's computer.

With respect to Claim 24, all the limitation is met by Atkinson et al except for the following limitation.

The limitation of "wherein the get trap and set trap commands identify a pointer to an original address and replace the original address with a new patch address" is met by Walsh on column 2, lines 6-13.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Walsh et al within the system of Atkinson et al so as to prevent a malicious program from being downloaded onto the client's computer.

Claims 9-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Atkinson et al (6367012 B1) in view of Chess (5572590).

With respect to Claim 9, all the limitation is met by Atkinson et al except for the limitation disclosed below.

The limitation of "wherein the action requested is a password manipulation" is met by Chess on column 1, lines 49-55 and on column 2, lines 8-13.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Chess within the system of Atkinson et al because a malicious change could be easily categorized as a password manipulation. Hence Chess's disclosure can be taken to cover a password manipulation.

With respect to Claim 10 and 11 all the limitation is met by Atkinson et al except for the limitation disclosed below.

The limitation of "wherein the action requested is deletion/modification of data" is met by Chess on column 1, lines 49-55 and column 2, lines 8-13.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Chess within the system of Atkinson et al because deletion/modification of data is a malicious change to data stored on a computer. Hence Chess's disclosure can be taken to mean deletion/modification of data.

With respect to Claim 12, all the limitation is met by Atkinson et al except for the limitation disclosed below.

The limitation of "wherein the action requested is manipulation of an operating system" is met by Chess on column 1, lines 49-55 and on column 2, lines 8-13.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Chess within the system of Atkinson et al because unauthorized manipulation of an operating system is a malicious change to data stored on a computer. Hence Chess's disclosure can be taken to mean manipulation of an operating system.

Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Atkinson et al (6367012 B1) in view of Szymanski et al (5574903).

With respect to Claim 21, all the limitation is met by Atkinson et al except for the following limitation.

The limitation of "wherein the creator code is a 4-byte value used to tie together a plurality of databases related to each application, at least one of the databases is maintained on the handheld computer using a first creator code that is the same as a second creator code associated with a plurality of patches, the at least one database contains a list of a plurality of the creator code resident on the handheld computer, and each creator code is used to prevent a program from modifying one of the databases with a different creator code" is met by Szymanski et al on column 7, lines 29-39 and in the abstract.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Szymanski et al within the system of Atkinson et al so as to allow for the proper allocation and execution of the called application.

Claims 7 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Atkinson et al (6367012 B1) in view of Blonder (5802275).

With respect to Claim 7, Atkinson et al meets the limitation of "receiving data on an infrared port of the handheld computer and installing said data in a temporary database" is met on column 2, lines 8-12. The sandbox/playpen provides a temporary storage database or medium for the suspicious program. The handheld device is obvious for the reasons disclosed in Claim 1. The infrared port is however not met by Atkinson et al. It is however disclosed by Blonder on column 1, lines 37-42.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Blonder within the system of Atkinson et al so as to ensure a prevent a malicious program from being downloaded to the client's computer.

With respect to Claim 22, Atkinson meets all the limitation except for the following limitation.

Blonder meets the limitation of "wherein a user has an option of disabling the detection of potentially harmful actions, specifying whether a plurality of databases scanned by a virus scanner are considered trusted if the virus scanner returns a favorable result" in the abstract; and "checking data that has entered the handheld computer through an infra-red (IR) port" on column 1, lines 37-42; and "specifying the trusted application" on column 1, lines 59-67; column 2, lines 1-3. Official notice is taken on the use of a password to turn on the handheld computer. This is already well known in the art and is used in various applications of client station screen-savers and Windows® screen lock systems. It would have been obvious to protect these passwords by

memorizing them or by not writing them down. If written down, they must be kept in a secure location.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Blonder within the system of Atkinson et al so as to ensure a prevent a malicious program from being downloaded to the client's computer.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tracey Akpati whose telephone number is 571-272-3846. The examiner can normally be reached on 8.30am-6.00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

OTA

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100